PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2004015077 A

(43) Date of publication of application: 15.01.04

(51) Int. CI

H04M 1/667

G06F 15/00

H04L 9/32

H04M 11/00

H04Q 7/38

(21) Application number: 2002161307

(71) Applicant:

MITSUBISHI ELECTRIC CORP

(22) Date of filing: 03.06.02

(72) Inventor:

MOCHIZUKI YASUYUKI

SUZUKI KENTA

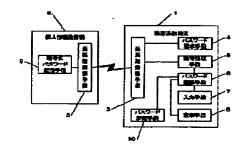
(54) SECURITY SYSTEM FOR PORTABLE COMMUNICATION TERMINAL AND ITS METHOD

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a security system for a portable communication terminal for reducing the load of password entry by a user while achieving access control with the password for the portable communication terminal, and for preventing the password from being stolen by someone else through the encryption of the password to be transmitted.

SOLUTION: A short range radio means 3 of a portable communication terminal 1 receives an encrypted password transmitted from the short range radio means 3 of a personal information transmitter 2, an encryption processing means 5 decrypts the password from the encrypted password, a password authenticating means 6 authenticates whether the decrypted password matches a pre-stored password, and an input means 7 accepts an input from the user when the password is authenticated by the password authentication means 6.

COPYRIGHT: (C)2004,JPO



(19) 日本国特許庁(JP)

(12) 公 開 特 許 公 報(A)

(11)特許出願公開番号

特開2004-15077 (P2004-15077A)

(43) 公開日 平成16年1月15日(2004.1.15)

(51) Int. C1. 7		FI				テーマコ・	ード(参考	 ≩)
HO4M	1/667	HO4M	1/667			5B08	5	
G06F	15/00	GO6F	15/00	330G		5 J 1 O	4	
H 04 L	9/32	HO4M	11/00 3	302		5K02	7	
HO4M	11/00	HO4L	9/00 €	373C		5K06	7	
H04Q	7/38	HO4B	7/26 1	109R		5K10	1	
			審査請求	未謂求	請求項の	O数 5 O	L (全	10 頁)
(21) 出願番号		特願2002-161307 (P2002-161307)	(71) 出願人	000006	013			
(22) 出願日		平成14年6月3日 (2002.6.3)		三菱電	费株式会社	生		
			東京都千代田区丸の内二丁目2番3号					号
			(74) 代理人 100102439					
				弁理士	宮田 会	金雄		
			(74) 代理人	100092	162			
					高瀬 引	用平		
			(72) 発明者		泰行			
							「目2番3	号 三
					株式会社内	勺		
			(72) 発明者	鈴木				
				-			「目2番3	号 三
			D		株式会社内	-	10 IDI-	4 DO O
			Fターム (参	·考() 5B0		AEO9 AE		AE29
					BC02	BEO1 BG		金字ノ
							最終頁に	म्राज्य ६

(54) 【発明の名称】携帯通信端末セキュリティシステム及びその方法

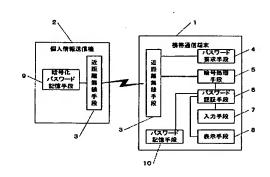
(57)【要約】

【課題】パスワードによる携帯通信端末へのアクセス制御を実現しながら利用者によるパスワード入力の負担を軽減し、また、送信するパスワードを暗号化することによりパスワードを他人に盗まれることのなり携帯通信端末セキュリティシステムを提供する。

【解決手段】携帯通信端末1の近距離無線手段3が個人精報送信機2の近距離無線手段3により送信された暗号化パスワードを受信し、暗号処理手段5が暗号化パスワードからパスワードを解読し、パスワード認証手段6が解読されたパスワードが予め格納されたパスワードと一致するが認証を行い、入力手段7がパスワード認証手段6によりパスワード認証がされた時に利用者からの入力を受け入れる。

【選択図】

図 1



【特許請求の範囲】

【請求項1】

暗号化パスワードが記憶された暗号化パスワード記憶手段と、パスワード要求時に前記暗号化パスワード記憶手段から取り出した暗号化パスワードを送信する第1の近距離無線手段とを有する個人情報送信機と、

前記第1の近距離無線手段にパスワード要求を送信し、又前記第1の近距離無線手段により送信された前記暗号化パスワードを受信する第2の近距離無線手段と、前記暗号化パスワードがよれ、フードを解読する暗号処理手段と、前記暗号処理手段により解読されたパスワードが予め格納されたパスワードと一致するが認証を行うパスワード認証手段と、前記パスワード認証手段によりパスワード認証がされた時に利用者がらの入力を受け入れる入力手段とを有する携帯通信端末と、を備えたことを特徴とする携帯通信端末セキュリティシステム。

【請求項2】

前記携帯通信端末は、前記パスワードの認証の有効期限が格納された自動パスワード認証 有効期限記憶手段を備え、

前記第2の近距離無線手段は、前記自動パスワード認証有効期限記憶手段に格納された有効期限が有効期限を過ぎていない時に前記第1の近距離無線手段にパスワード要求を送信することを特徴とする請求項1記載の携帯通信端末セキュリティシステム。

【請求項3】

前記個人精報送信機は、通常モードと紛失モードとのモード精報を格納するモード記憶手 段を備え、

前記第1の近距離無線手段は、前記モード橋報が通常モードの時は前記第2の近距離無線手段に前記暗号化パスワードを送信し、又前記モード橋報が紛失モードの時は前記第2の近距離無線手段に前記暗号化パスワードを送信しないことを特徴とする請求項1記載の携帯通信端末セキュリティシステム。

【請求項4】

前記個人情報送信機は、アラーム動作させるアラーム手段を備え、

前記第1の近距離無線手段は、前記第2の近距離無線手段に前記暗号化パスワードを送信しない時に上記アラーム手段にアラーム動作させることを特徴とする請求項3記載の携帯通信端末セキュリティシステム。

【請求項5】

暗号化パスワードが記憶された個人情報送信機に近距離無線手段を介してパスワード要求を送信する送信ステップと、前記送信ステップによりパスワード要求を送信した後に前記個人情報送信機から近距離無線手段を介して前記暗号化パスワードを受信する受信ステップと、前記受信ステップにより受信された前記暗号化パスワードがより、マードを解読する暗号処理ステップと、前記暗号処理ステップにより解読されたパスワードが予め格納されたパスワードと一致するが認証を行うパスワード認証ステップと、前記パスワード認証がされた時に利用者からの入力を受け入れる入力ステップと、を備えたことを特徴とする携帯通信端末セキュリティ方法。

【発明の詳細な説明】

[0001]

【発明の属する技術分野】

この発明は、盗難、紛失などにより携帯通信端末が意図せずに他人の手に渡った際のセキュリティに関するものである。

[0002]

【従来の技術】

従来の携帯電話は、盗難や紛失時の惡用対策として、パスワードによるアクセス制御を行なっていた。これはあらかしめ携帯電話にパスワードを設定し、携帯電話から電話をかけたり、住所録などの個人情報にアクセスしたりする前に、利用者に対してパスワード入力を要求し、正しいパスワードが入力された場合にのみ通話機能や住所録情報へのアクセス

50

40

10

20

30

Patent provided by Sughrue Mion, PLLC - http://www.sughrue.com

制限を解除するというものであった。

【発明が解決しようとする課題】

[0003]

従来の携帯電話では、通信機能を利用したり住所録などの個人情報にアクセスしたりする たびに、利用者が何度もパスワードを入力する必要があるという問題点があった。また、 パスワードの入力操作を他人に見られると、パスワードが盗まれるという問題点があった

[0004]

この発明は上記のような問題点を解決するためになされたもので、個人情報送信機にパスワードを記憶させ、近距離無線を使って自動的にパスワードを送信することにより、パスワードによる携帯通信端末へのアクセス制御を実現しながら利用者によるパスワード入力の負担を軽減し、また、送信するパスワードを暗号化することによりパスワードを他人に盗まれる可能性を低くすることを目的とする。

[0005]

【課題を解決するための手段】

第 1 の 発明は、 暗号 化 パス ワード が 記 檍 さ れ 友 暗 号 化 パス ワード 記 檍 手 段 と 、 パス ワード 要 求 時 に 前 記 暗 号 化 パス ワード 記 檍 手 段 か ら 取 り 出 し 友 暗 号 化 パス ワード を 送 信 す る 第 1 の 近 距 離 無 線 手 段 と を 有 す る 個 人 精 報 送 信 機 と 、

前記第1の近距離無線手段にパスワード要求を送信し、又前記第1の近距離無線手段により送信された前記暗号化パスワードを受信する第2の近距離無線手段と、前記暗号化パスワードからパスワードを解読する暗号処理手段と、前記暗号処理手段により解読されたパスワードが予め格納されたパスワードと一致するか認証を行うパスワード認証手段と、前記パスワード認証手段によりパスワード認証がされた時に利用者からの入力を受け入れる入力手段とを有する携帯通信端末とを備えたものである。

[0006]

第2の発明は、前記パスワードの認証の有効期限が格納された自動パスワード認証有効期限記憶手段を有する携帯通信端末と、

前記自動パスワード認証有効期限記憶手段に格納された有効期限が有効期限を過ぎていない時に前記第1の近距離無線手段にパスワード要求を送信する第2の近距離無線手段とを備えたものである。

[0007]

第3の発明は、通常モードと紛失モードとのモード情報を格納するモード記憶手段を有する個人精報送信機と、

前記モード情報が通常モードの時は前記第2の近距離無線手段に前記暗号化バスワードを送信し、又前記モード情報が紛失モードの時は前記第2の近距離無線手段に前記暗号化バスワードを送信しなり第1の近距離無線手段とを備えたものである。

[0008]

第4の発明は、アラーム動作させるアラーム手段を有する個人精報送信機と、前記第2の近距離無線手段に前記暗号化パスワードを送信しない時に上記アラーム手段にアラーム動作させる第1の近距離無線手段とを備えたものである。

[0009]

第5の発明は、暗号化パスワードが記憶された個人情報送信機に近距離無線手段を介してパスワード要求を送信する送信ステップと、前記送信ステップによりパスワード要求を送信する送信ステップと、前記送信ステップによりで記暗号化パスワードを受信する受信ステップと、前記受信ステップにより受信された前記暗号化パスワードからパスワードを解読する暗号処理ステップと、前記暗号処理ステップにより解読されたパスワードが予め格納されたパスワードと一致するか認証を行うパスワード認証ステップと、前記パスワード認証ステップと、前記パスワード認証ステップとを備えたものである。

[0010]

50

10

20

30

【発明の実施の形態】

実施の形態 1.

図1は、実施の形態1の携帯通信端末セキュリティシステムの構成図である。図1において、1は携帯通信端末、2は個人精報送信機、3は近距離無線手段、4はパスワード要求手段、5は暗号処理手段、6はパスワード認証手段、7は入力手段、8は表示手段、9は暗号化パスワード記憶手段、10はパスワード記憶手段である。近距離通信手段3は携帯通信端末1と個人精報送信機2に共通に備えられており、携帯通信端末1と個人精報送信機2とは近距離通信手段3を用いて通信を行なう。

[0011]

次に、動作について示す。

図 2 は、実施の形態 1 の携帯通信端末セキュリティシステムの処理動作を示す流れ図である。

まず、携帯通信端末1においてパスワードが要求されると、パスワード要求手段4においてパスワード要求メッセージが生成され、近距離無線手段3から送信される(ステップ82)。次に、個人精報送信機2において近距離無線手段3でパスワード要求メッセージを受信すると(ステップ83)、暗号化パスワード記憶手段9から暗号化パスワードが取り出され(ステップ84)、近距離無線手段3から携帯通信端末1に暗号化パスワードが送信される(ステップ85)。

[0012]

携帯通信端末1は、個人精報送信機2の近距離無線手段3から送信される暗号化パスワードの受信待で状態となり(ステップ86)、パスワード受信に失敗すると(ステップ821)、表示手段8にパスワード入力を促すメッセージを表示する(ステップ811)。 一方、パスワード受信に成功すると(ステップ821)、暗号処理手段5により暗号化パスワードの解読が行なわれてパスワードが取り出され(ステップ87)、パスワード認証手段6によって正当性の検証が実行される(ステップ88)。

[0013]

パスワードの正当性の検証では、パスワード記憶手段10に格納されているパスワードを取り出し、解読したパスワードと一致するか否かの検証をする。解読されたパスワードの認証が成功すれば(ステップ89)、入力制限を解除して(ステップ810)、利用者による入力手段7からの入力を受け入れる。

また、解読されたパスワードの認証が失敗すれば(ステップ S 9)、表示手段 8 にパスワード入力を促すメッセージを表示し(ステップ S 1 1)、入力手段 7 から入力されるパスワードを読み込んで(ステップ S 1 2)、パスワード認証手段 6 によって正当性の検証が実行される(ステップ S 1 3)。

[0014]

ここで、入力されたパスワードの認証が成功すれば(ステップ814)、入力制限を解除して(ステップ810)、入力手段7からの入力を受け入れる。また、入力されたパスワードの認証が失敗すれば(ステップ814)、入力制限を実施して(ステップ815)、入力手段7からの入力を受け入れない。

[0015]

以上のように本実施の形態によれば、携帯通信端末1においてパスワードを要求する事象が発生した際に、個人情報送信機2からパスワード情報を自動的に取得してパスワード認証を行なうので、利用者によるパスワード入力が省略されて利便性が高まるという効果、および、パスワード入力操作を他人に見られることによるパスワードの盗難を防止できるという効果が得られる。

[0016]

また、もし個人情報送信機2との間の近距離無線による通信路が確立されなければ、パスワード機報が自動的には取得できないため、パスワードが携帯通信端末1に入力されない限り携帯通信端末1への入力が制限され、携帯通信端末1の紛失や盗難においても他人が不正に通信機能を使用することを防止できるという効果が得られる。

50

40

10

20

[0017]

さらに、個人精報送信機 2 に記憶するパスワードをあらかしめ暗号化することにより、個人精報送信機が盗難にあっったり、無線通信が傍受されても、パスワードを盗まれることを防止できるという効果が得られる。

[0018]

また、携帯通信端末1が個人精報送信機2からパスワード精報を受信できなくても、携帯通信端末1にパスワードを入力することによって入力制限が解除されるので、個人精報送信機1の故障や紛失が発生しても携帯通信端末1は継続して使用できるという効果がある

[0019]

また、パスワード認証を入力制限に適用する代わりに、通信機能へのアクセス制限やプライペート精報や課金情報へのアクセス制限に適用しても同様の効果を得ることができる。 【 0 0 2 0 】

実施の形態 2.

図3は、実施の形態2の携帯通信端末セキュリティシステムの構成図であり、図1と同一符号は同一又は相当部分を示し説明を省略する。

図 3 に お い て 、 1 1 は 自 動 パ ス ワ ー ド 認 証 有 効 期 限 記 様 手 段 で あ る 。 自 動 パ ス ワ ー ド 認 証 有 効 期 限 記 様 手 段 1 1 に は 、 個 人 橋 報 送 信 機 2 を 利 用 し た 自 動 的 な パ ス ワ ー ド 認 証 の 有 効 期 限 が 格 納 さ れ る 。

υ

[0021]

次に、動作について示す。

図 4 は、実施の形態 2 の携帯通信端末セキュリティシステムの処理動作を示す流れ図である。

まず、携帯通信端末1においてパスワードが要求されると、自動パスワード認証有効期限記憶手段11に格納されている有効期限から、自動パスワード認証の有効期限を確認する(ステップ816)。有効期限を過ぎている場合は(ステップ817)、表示手段8にパスワード入力を促すメッセージを表示する(ステップ811)。また、自動パスワード認証の有効期限を過ぎていない場合は(ステップ817)、パスワード要求手段4においてパスワード要求メッセージが近距離無線手段3から個人情報送信機2に送信される(ステップ82)。

[0022]

次に、個人情報送信機2において携帯通信端末1の近距離無線手段3から送信されたパスワード要求メッセージを受信すると(ステップ33)、パスワード記憶手段9から暗号化パスワードが取り出され(ステップ34)、近距離無線手段3から携帯通信端末1に暗号化パスワードが送信される(ステップ35)。

[0023]

携帯通信端末1は、個人精報送信機2の近距離無線手段3から送信される暗号化パスワードの受信待ち状態となり(ステップ36)、パスワード受信に失敗すると(ステップ32 1)、表示手段8にパスワード入力を促すメッセージを表示(ステップ31)する。

一方、パスワード受信に成功すると(ステップ821)、暗号処理手段5により暗号化パスワードの解読が行なわれてパスワードが取り出され(ステップ87)、パスワード認証手段6によって正当性の検証が実行される(ステップ88)。

[0024]

パスワードの正当性の検証では、パスワード記憶手段10に格納されているパスワードを取り出し、解読したパスワードと一致するか否かの検証をする。解読されたパスワードの認証が成功すれば(ステップ89)、入力制限を解除して(ステップ810)、入力手段 7からの入力を受け入れる。

また、解読されたパスワードの認証が失敗すれば(ステップ89)、表示手段8にパスワード入力を促すメッセージを表示し(ステップ811)、入力手段7から入力されるパスワードを読み込んで(ステップ812)、パスワード認証手段6によって正当性の検証が

50

10

20

30

実行される(ステップ81.3)。

[0025]

ここで、入力されたパスワードの認証が成功すれば(ステップ 8 1 4)、自動パスワード認証の新たな有効期限を設定し、この自動パスワード認証の新たな有効期限を自動パスワード認証有効期限記憶手段 1 1 に格納し(ステップ 8 1 8)、入力制限を解除して(ステップ 8 1 0)、入力手段 7 からの入力を受け入れる。また、入力されたパスワードの認証が失敗すれば(ステップ 8 1 4)、入力制限を実施して(ステップ 8 1 5)入力手段 7 からの入力を受け入れない。

[0026]

以上のように本実施の形態によれば、自動パスワード認証に有効期限を設け、自動パスワード認証が有効でなくなったらユーザにパスワード入力を要求するので、携帯通信端末1を個人精報送信機2とともに紛失したり盗難されたりしても、有効期限を過ぎると自動的に携帯通信端末1が利用できなくなり、携帯通信端末の不正利用ができなくなるという効果がある。

[0027]

また、バスワード認証を入力制限に適用する代わりに、通信機能へのアクセス制限やプライベート情報や課金情報へのアクセス制限に適用しても同様の効果を得ることができる。 【 0 0 2 8 】

実施の形態3.

図 5 は、実施の形態 3 の携帯通信端末セキュリティシステムの構成図であり、図 1 と同一符号は同一又は相当部分を示し説明を省略する。

図5において、12はモード切替手段、13はモード記憶手段、14はアラーム手段である。モード記憶手段13には「通常モード」と「紛失モード」の2つのモードのいずれかであることが記憶される。

[0029]

次に、動作について示す。

図 6 は、実施の形態 3 の携帯通信端末セキュリティシステムの処理動作を示す流れ図である。

まず、携帯通信端末セキュリティシステムの処理動作の前に、利用者は個人情報送信機2のモード切替手段12によって「通常モード」と「紛失モード」のいずれかを選択する。モード切替手段12によって選択されたモードは、モード記憶手段13にモード情報として格納される。

[0030]

個人精報送信機2は、携帯通信端末1の近距離無線手段3から送信されたパスワード要求メッセージを受信すると(ステップ83)、モード記憶手段13からモード情報を取り出し、モード情報が「紛失モード」の場合は(ステップ822)、アラーム手段14に通知してアラームを動作させ(ステップ823)、暗号化パスワードの送信は行なわない。また、モード情報が「通常モード」の場合は(ステップ822)、パスワード記憶手段9から暗号化パスワードが取り出され(ステップ84)、近距離無線手段3から携帯通信端末1に暗号化パスワードが送信される(ステップ85)。以後の処理は実施の形態1や実施の形態2と同様である。

[0031]

以上のように本実施の形態によれば、個人情報送信機に「通常モード」と「紛失モード」の二つのモードを設け、「紛失モード」の場合に暗号化パスワードの送信を行なわず利用者にアラームを行なうことにより、利用者が紛失したと思っている携帯通信端末が利用者の知らない間に個人情報送信機の近辺で不正に利用されることを防ぎ、さらに紛失した携帯通信端末が個人情報送信機の近辺に存在することを利用者に認知させることができるという効果がある。

[0082]

【発明の効果】

50

10

20

30

10

20

30

40

50

この発明は、以上説明したように構成されているので、以下に示すような効果を奏する。 【0033】

第1の発明では、携帯通信端末の第2の近距離無線手段が個人精報送信機の第1の近距離無線手段により送信された暗号化パスワードを受信し、暗号処理手段が暗号化パスワードがあり、カスワードを開読し、パスワード認証手段が解読されたパスワードが予め格納されたパスワードと一致するか認証を行い、入力手段がパスワード認証手段によりパスワード認証手段によりパスワード認証がされた時に利用者からの入力を受け入れることにより、利用者によるパスワード入力が省略されるので利用者の利便性を高めることができる。またパスワード入力操作を他人に見られることがないのでパスワードの盗難を防止することができる。

[0034]

第2の発明では、携帯通信端末の第2の近距離無線手段が、自動パスワード認証有効期限記憶手段に格納された有効期限が期限内である時に第1の近距離無線手段にパスワード要求を送信することにより、携帯通信端末を個人情報送信機とともに紛失したり盗難されたりしても、有効期限を過ぎると自動的に携帯通信端末が利用できなくなるので、携帯通信端末の不正利用を防止することができる。

[0035]

第3の発明では、個人情報送信機のモード記憶手段に格納されたモード情報が通常モードの時は、携帯通信端末の第2の近距離無線手段に暗号化パスワードを送信し、又モード情報が紛失モードの時は携帯通信端末の第2の近距離無線手段に暗号化パスワードを送信しないようにすることにより、利用者が紛失したと思っている携帯通信端末が利用者の知らない間に個人情報送信機の近辺で不正に利用されることを防ぐことができる。

[0036]

第4の発明では、個人情報送信機の第1の近距離無線手段が第2の近距離無線手段に暗号化パスワードを送信しない時にアラーム手段にアラーム動作させることにより、紛失した携帯通信端末が個人情報送信機の近辺に存在することを利用者に認知させることができる

[0037]

【図面の簡単な説明】

【図1】実施の形態1の携帯通信端末セキュリティシステムの構成図。

【図2】実施の形態1における携帯通信端末セキュリティシステムの処理動作を示す流れ図。

【 図 3 】 実 施 の 形 態 2 の 携 帯 通 信 端 末 セ キ ュ リ テ ィ シ ス テ ム の 構 成 図 。

【図4】実施の形態2における携帯通信端末セキュリティシステムの処理動作を示す流れ図。

【 図 5 】 実 施 の 形 態 3 の 携 帯 通 信 端 末 セ キ ュ リ テ ィ シ ス テ ム の 構 成 図 。

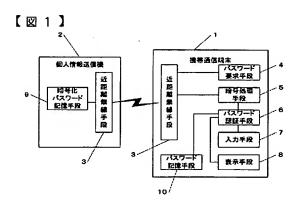
【図 6 】実施の形態 3 における携帯通信端末セキュリティシステムの処理動作を示す流れ図。

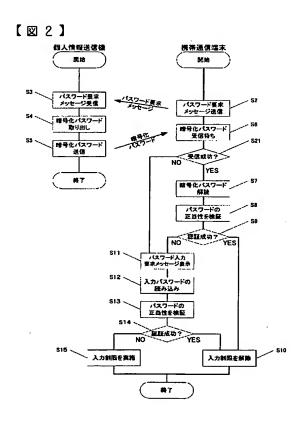
【符号の説明】

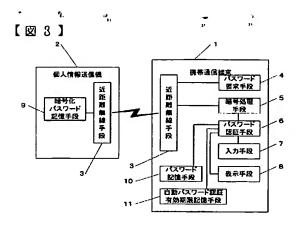
1 携帯通信端末、2 個人精報送信機、3 近距離無線手段、4 パスワード要求手段 、5 暗号処理手段、6 パスワード認証手段、7 入力手段、8 表示手段、9 暗号

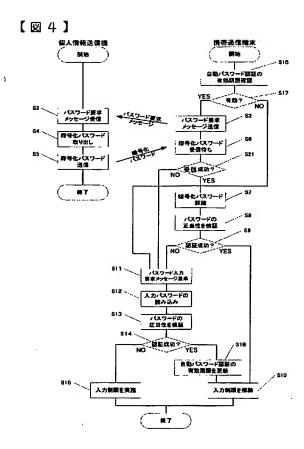
Patent provided by Sughrue Mion, PLLC - http://www.sughrue.com

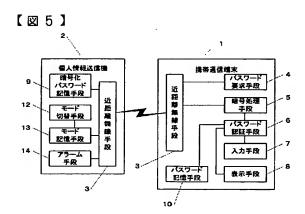
化パスワード記憶手段、1°0 パスワード記憶手段、11 自動パスワード認証有効期限記憶手段、12 モード切替手段、13 モード記憶手段、14 アラーム手段。

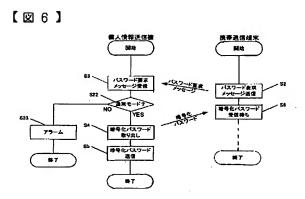












フロントページの続き

Fターム(参考) 5J104 AA07 KA01 NA05 PA02

5K027 AA11 BB09 HH24

5K067 AA32 AA34 DD17 FF18 FF31 GG01 HH22 HH23 HH24

5K101 LL12

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

□ BLACK BORDERS
□ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
□ FADED TEXT OR DRAWING
□ BLURRED OR ILLEGIBLE TEXT OR DRAWING
□ SKEWED/SLANTED IMAGES
□ COLOR OR BLACK AND WHITE PHOTOGRAPHS
□ GRAY SCALE DOCUMENTS
□ LINES OR MARKS ON ORIGINAL DOCUMENT
□ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

IMAGES ARE BEST AVAILABLE COPY.

☐ OTHER:

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.